Dowd 3-3

1. A method of accessing an information processing network, comprising the steps of:

a) initializing a database, an approved list, and a disapproved list, where the database contains rules for allowing and denying access to the information processing network, where the approved list includes approvals of connectionless network packets, and where the disapproved list includes disapprovals of connectionless network packets;

b) receiving a connectionless network packet;

c) computing a flow tag based on the connectionless network packet;

d) discarding the connectionless network packet and returning to step (b) if the flow tag is on the disapproved list;

e) allowing the connectionless network packet access to the information processing network and returning to step (b) if the flow tag is on the approved list;

f) comparing the flow tag to the database if the flow tag is not on the approved list and is not on the disapproved list;

g) discarding the connectionless network packet, adding the flow tag to the disapproved list, and returning to step (b) if the database rejects the flow tag; and

h) allowing the connectionless network packet access to the information processing network, adding the flow tag to the approved list, and returning to step (b) if the database accepts the flow tag.

2. The method of claim 1, wherein said step of computing a flow tag is comprised of the steps of:

a) extracting from the connectionless network packet a user-definable number of bits from a connectionless network source address, a connectionless network destination address, a

connectionless network protocol, an upper layer protocol header if included in the connectionless network packet, and application layer data;

b) substituting all zeros for the upper layer protocol layer if none is included in the connectionless network packet;

c) setting a user-definable number and location of bits in the result of the last step to zero; and

d) computing a flow tag address.

3. The method of claim 2, where said step of computing a flow tag address is comprised of the steps of:

a) setting a zeroth bit of the flow tag address to $f_0 = s_0 \times s_{14} \times s_{28} \times d_{13} \times d_{27} \times h_0 \times h_{16}$, where x is a bitwise exclusive-or operation, f_i is the ith bit of the flow tag address, where s_i is the ith bit of a connectionless network source address, where d_i is the ith bit of a connectionless network destination address, where p_i is the ith bit of a connectionless network protocol, and where h_i is the ith bit of the upper layer protocol header, and;

b) setting a first bit of the flow tag address to $f_1 = s_1 \times s_{15} \times s_{29} \times d_{12} \times d_{26} \times h_1 \times h_{17}$;

c) setting a second bit of the flow tag address to $f_2 = s_2 \times s_{16} \times s_{30} \times d_{11} \times d_{25} \times h_2 \times h_{18} \times p_0$;

d) setting a third bit of the flow tag address to $f_3 = s_3 \times s_{17} \times s_{31} \times d_{10} \times d_{24} \times h_3 \times h_{19} \times p_1$;

e) setting a fourth bit of the flow tag address to $f_4 = s_4 \times s_{18} \times d_9 \times d_{23} \times h_4 \times h_{20} \times p_2$;

f) setting a fifth bit of the flow tag address to $f_5 = s_5 \times s_{19} \times d_8 \times d_{22} \times h_5 \times h_{21} \times p_3$;

g) setting a sixth bit of the flow tag address to $f_6 = s_6 \times s_{20} \times d_7 \times d_{21} \times h_6 \times h_{22} \times h_{28} \times p_4$;

h) setting a seventh bit of the flow tag address to $f_7 = s_7 \times s_{21} \times d_6 \times d_{20} \times h_7 \times h_{23} \times h_{29} \times p_5$;

i) setting a eighth bit of the flow tag address to $f_8 = s_8 \times s_{22} \times d_5 \times d_{19} \times h_8 \times h_{24} \times h_{30} \times p_6$;

j) setting a ninth bit of the flow tag address to $f_9 = s_9 \times s_{23} \times d_4 \times d_{18} \times h_9 \times h_{25} \times h_{31} \times p_7$;

k) setting a tenth bit of the flow tag address to $f_{10} = s_{10} \times s_{24} \times d_3 \times d_{17} \times d_{31} \times h_{10} \times h_{26}$;

l) setting a eleventh bit of the flow tag address to $f_{11} = s_{11} \times s_{25} \times d_2 \times d_{16} \times d_{30} \times h_{11} \times h_{27}$;

m) setting a twelfth bit of the flow tag address to $f_{12} = s_{12} \times s_{26} \times d_1 \times d_{15} \times d_{29} \times h_{12} \times h_{14}$; and

n) setting a thirteenth bit of the flow tag address to $f_{13} = s_{13} \times s_{27} \times d_0 \times d_{14} \times d_{28} \times h_{13} \times h_{15}$.

4. The method claim 1, wherein the step of discarding the connectionless network packet, adding the flow tag to the disapproved list, and returning to step (b) if the database rejects the flow tag is comprised of the steps of:

a) comparing the flow tag to any data stored on the disapproved list at the flow tag address;

b) determining that the flow tag is on the disapproved list if a match occurred in the last step;

c) discarding the connectionless network packet;

d) adding the flow tag to the disapproved list; and

e) returning to step (b).

5. The method claim 1, wherein the step of allowing the connectionless network packet access to the information processing network, adding the flow tag to the approved list, and returning to step (b) if the database accepts the flow tag is comprised of the steps of:

a) comparing the flow tag to any data stored on the approved list at the flow tag address;

b) determining that the flow tag is on the approved list if a match occurred in the last step;

c) allowing the connectionless network packet access to the information processing network;

d) adding the flow tag to the approved list; and

e) returning to step (b).

6. The method of claim 1, further including the step of recording all allowances of access to the information processing network and recording all discarded connectionless network packets.

7. The method of claim 6, further including the step of alerting a system administrator if the number of discarded connectionless network packets exceed a user-definable threshold.

8. The method of claim 6, further including the step of alerting a system administrator if the number of discarded connectionless network packets exceed a user-definable threshold within a user-definable span of time.

9. The method claim 3, wherein the step of discarding the connectionless network packet, adding the flow tag to the disapproved list, and returning to step (b) if the database rejects the flow tag is comprised of the steps of:

a) comparing the flow tag to any data stored on the disapproved list at the flow tag address;

b) determining that the flow tag is on the disapproved list if a match occurred in the last step;

c) discarding the connectionless network packet;

d) adding the flow tag to the disapproved list; and

e) returning to step (b).

10. The method claim 9, wherein the step of allowing the connectionless network packet access to the information processing network, adding the flow tag to the approved list, and returning to step (b) if the database accepts the flow tag is comprised of the steps of:

a) comparing the flow tag to any data stored on the approved list at the flow tag address;

b) determining that the flow tag is on the approved list if a match occurred in the last step;

c) allowing the connectionless network packet access to the information processing network;

d) adding the flow tag to the approved list; and

e) returning to step (b).

11. The method of claim 10, further including the step of recording all allowances of access to the information processing network and recording all discarded connectionless network packets.

12. The method of claim 11, further including the step of alerting a system administrator if the number of discarded connectionless network packets exceed a user-definable threshold.

13. The method of claim 11, further including the step of alerting a system administrator if the number of discarded connectionless network packets exceed a user-definable threshold within a user-definable span of time.

14. A method of accessing an information processing network, comprising the steps of:

a) initializing a database, an approved list, and a disapproved list, where the database contains rules for allowing and denying access to the information processing network, where the approved list includes approvals of IP packets, and where the disapproved list includes disapprovals of IP packets;

b) receiving an IP packet;

c) computing a flow tag based on the IP packet;

d) discarding the IP packet and returning to step (b) if the flow tag is on the disapproved list;

e) allowing the IP packet access to the information processing network and returning to step (b) if the flow tag is on the approved list;

f) comparing the flow tag to the database if the flow tag is not on the approved list and is not on the disapproved list;

g) discarding the IP packet, adding the flow tag to the disapproved list, and returning to step (b) if the database rejects the flow tag; and

h) allowing the IP packet access to the information processing network, adding the flow tag to the approved list, and returning to step (b) if the database accepts the flow tag.

15. The method of claim 14, wherein said step of computing a flow tag is comprised of the steps of:

a) extracting from the IP packet a user-definable number of bits from a IP source address, a IP destination address, a IP protocol, an upper layer protocol header if included in the IP packet, and data;

b) substituting all zeros for the upper layer protocol layer if none is included in the IP packet;

c) setting a user-definable number and location of bits in the result of the last step to zero; and

d) computing a flow tag address.

16. The method of claim 15, where said step of computing a flow tag address is comprised of the steps of:

a) setting a zeroth bit of the flow tag address to $f_0 = s_0 \times s_{14} \times s_{28} \times d_{13} \times d_{27} \times h_0 \times h_{16}$, where x is a bitwise exclusive-or operation, f_i is the ith bit of the flow tag address, where s_i is the ith bit of a IP source address, where d_i is the ith bit of a IP destination address, where p_i is the ith bit of a IP protocol, and where h_i is the ith bit of the upper layer protocol header, and;

b) setting a first bit of the flow tag address to $f_1 = s_1 \times s_{15} \times s_{29} \times d_{12} \times d_{26} \times h_1 \times h_{17}$;

c) setting a second bit of the flow tag address to $f_2 = s_2 \times s_{16} \times s_{30} \times d_{11} \times d_{25} \times h_2 \times h_{18} \times p_0$;

d) setting a third bit of the flow tag address to $f_3 = s_3 \times s_{17} \times s_{31} \times d_{10} \times d_{24} \times h_3 \times h_{19} \times p_1$;

e) setting a fourth bit of the flow tag address to $f_4 = s_4 \times s_{18} \times d_9 \times d_{23} \times h_4 \times h_{20} \times p_2$;

f) setting a fifth bit of the flow tag address to $f_5 = s_5 \times s_{19} \times d_8 \times d_{22} \times h_5 \times h_{21} \times p_3$;

g) setting a sixth bit of the flow tag address to $f_6 = s_6 \times s_{20} \times d_7 \times d_{21} \times h_6 \times h_{22} \times h_{28} \times p_4$;

h) setting a seventh bit of the flow tag address to $f_7 = s_7 \times s_{21} \times d_6 \times d_{20} \times h_7 \times h_{23} \times h_{29} \times p_5$;

i) setting a eighth bit of the flow tag address to $f_8 = s_8 \times s_{22} \times d_5 \times d_{19} \times h_8 \times h_{24} \times h_{30} \times p_6$;

j) setting a ninth bit of the flow tag address to $f_9 = s_9 \times s_{23} \times d_4 \times d_{18} \times h_9 \times h_{25} \times h_{31} \times p_7$;

k) setting a tenth bit of the flow tag address to $f_{10} = s_{10} \times s_{24} \times d_3 \times d_{17} \times d_{31} \times h_{10} \times h_{26}$;

l) setting a eleventh bit of the flow tag address to $f_{11} = s_{11} \times s_{25} \times d_2 \times d_{16} \times d_{30} \times h_{11} \times h_{27}$;

m) setting a twelfth bit of the flow tag address to $f_{12} = s_{12} \times s_{26} \times d_1 \times d_{15} \times d_{29} \times h_{12} \times h_{14}$; and

n) setting a thirteenth bit of the flow tag address to $f_{13} = s_{13} \times s_{27} \times d_0 \times d_{14} \times d_{28} \times h_{13} \times h_{15}$.

17. The method claim 14, wherein the step of discarding the IP packet, adding the flow tag to the disapproved list, and returning to step (b) if the database rejects the flow tag is comprised of the steps of:

a) comparing the flow tag to any data stored on the disapproved list at the flow tag address;

b) determining that the flow tag is on the disapproved list if a match occurred in the last step;

c) discarding the IP packet;

d) adding the flow tag to the disapproved list; and

e) returning to step (b).

18. The method claim 14, wherein the step of allowing the IP packet access to the information processing network, adding the flow tag to the approved list, and returning to step (b) if the database accepts the flow tag is comprised of the steps of:

a) comparing the flow tag to any data stored on the approved list at the flow tag address;

b) determining that the flow tag is on the approved list if a match occurred in the last step;

c) allowing the IP packet access to the information processing network;

d) adding the flow tag to the approved list; and

e) returning to step (b).

19. The method of claim 14, further including the step of recording all allowances of access to the information processing network and recording all discarded IP packets.

20. The method of claim 19, further including the step of alerting a system administrator if the number of discarded IP packets exceed a user-definable threshold.

21. The method of claim 19, further including the step of alerting a system administrator if the number of discarded IP packets exceed a user-definable threshold within a user-definable span of time.

22. The method claim 16, wherein the step of discarding the IP packet, adding the flow tag to the disapproved list, and returning to step (b) if the database rejects the flow tag is comprised of the steps of:

a) comparing the flow tag to any data stored on the disapproved list at the flow tag address;

b) determining that the flow tag is on the disapproved list if a match occurred in the last step;

c) discarding the IP packet;

d) adding the flow tag to the disapproved list; and

e) returning to step (b).

23. The method claim 22, wherein the step of allowing the IP packet access to the information processing network, adding the flow tag to the approved list, and returning to step (b) if the database accepts the flow tag is comprised of the steps of:

a) comparing the flow tag to any data stored on the approved list at the flow tag address;

b) determining that the flow tag is on the approved list if a match occurred in the last step;

c) allowing the IP packet access to the information processing network;

d) adding the flow tag to the approved list; and

e) returning to step (b).

24. The method of claim 23, further including the step of recording all allowances of access to the information processing network and recording all discarded IP packets.

25. The method of claim 24, further including the step of alerting a system administrator if the number of discarded IP packets exceed a user-definable threshold.

26. The method of claim 24, further including the step of alerting a system administrator if the number of discarded IP packets exceed a user-definable threshold within a user-definable span of time.

27. A device for accessing an information processing network, comprising:

a) a flow management unit, having a first input/output bus for receiving a flow, having a second input/output bus for transmitting the flow, and having a third input/output bus;

b) a first connectionless network flow processor, connected to the third input/output bus of said flow management unit, and having an input/output bus;

c) an approved list storage unit, connected to the input/output bus of said first connectionless network flow processor;

d) a disapproved list storage unit, connected to the input/output bus of said first connectionless network flow processor;

e) a flow command processor, connected to the third input/output bus of said flow management unit, and having an input/output bus;

f) a second connectionless network flow processor, connected to the input/output bus of said flow command processor, and having an input/output bus;

g) a connectionless network address database unit, connected to the input/output bus of said second connectionless network flow processor;

h) a memory management unit, connected to the third input/output bus of said flow management unit, and having an input/output bus; and

i) a memory unit, connected to the input/output bus of said memory management unit.